

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/004211

International filing date: 10 March 2005 (10.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-073335  
Filing date: 15 March 2004 (15.03.2004)

Date of receipt at the International Bureau: 14 July 2005 (14.07.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

23.06.2005

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 4 年   3 月 1 5 日  
Date of Application:

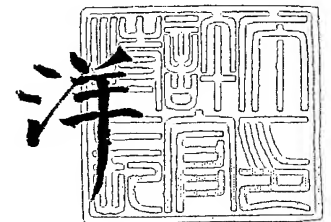
出 願 番 号            特 願 2 0 0 4 - 0 7 3 3 3 5  
Application Number:  
[ST. 10/C] :            [ J P 2 0 0 4 - 0 7 3 3 3 5 ]

出   願   人            オムロン株式会社  
Applicant(s):

2 0 0 5 年   3 月 1 1 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



出証番号   出証特 2 0 0 5 - 3 0 2 1 3 3 1

【書類名】 特許願  
【整理番号】 62847  
【提出日】 平成16年 3月15日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G08B 13/00  
【発明者】  
    【住所又は居所】 京都府京都市下京区塩小路通堀川東入南不動堂町 8 0 1 番地 オムロン株式会社内  
    【氏名】 太田 俊二  
【発明者】  
    【住所又は居所】 京都府京都市下京区塩小路通堀川東入南不動堂町 8 0 1 番地 オムロン株式会社内  
    【氏名】 中村 明彦  
【発明者】  
    【住所又は居所】 京都府京都市下京区塩小路通堀川東入南不動堂町 8 0 1 番地 オムロン株式会社内  
    【氏名】 久保田 正純  
【発明者】  
    【住所又は居所】 京都府京都市下京区塩小路通堀川東入南不動堂町 8 0 1 番地 オムロン株式会社内  
    【氏名】 竹内 寿  
【発明者】  
    【住所又は居所】 京都府京都市下京区塩小路通堀川東入南不動堂町 8 0 1 番地 オムロン株式会社内  
    【氏名】 向川 信一  
【発明者】  
    【住所又は居所】 京都府京都市下京区塩小路通堀川東入南不動堂町 8 0 1 番地 オムロン株式会社内  
    【氏名】 小林 秀行  
【特許出願人】  
    【識別番号】 000002945  
    【氏名又は名称】 オムロン株式会社  
【代理人】  
    【識別番号】 100080034  
    【弁理士】  
    【氏名又は名称】 原 謙三  
    【電話番号】 06-6351-4384  
【手数料の表示】  
    【予納台帳番号】 003229  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 0101830

**【書類名】 特許請求の範囲****【請求項 1】**

監視領域への不正侵入者を威嚇する威嚇処理を実行可能な外部の威嚇実行手段に対して威嚇処理の実行命令を付与する侵入者検知装置において、

自身が送波したマイクロ波が被検知物により反射されて生成される反射波における周波数の変化を測定することで、移動している物体を検知するドップラーセンサーと、

自身の外部と通信可能な通信手段と、

上記ドップラーセンサーにより上記反射波における周波数の変化が測定されたか否かを示す情報に基づき生成される情報であって、移動している物体があるか否かを示す移動物体有無情報に基づき、上記通信手段とユーザにより携帯される携帯端末との通信により、該携帯端末に予め登録されたユーザを特定することが可能な携帯端末側 ID 情報を読み出すとともに、上記侵入者検知装置内に予め登録されたユーザを特定することが可能な侵入者検知装置側 ID 情報と、上記携帯端末側 ID 情報とを照合することによって、上記物体がユーザであるか否かを識別する認証処理手段と、

上記侵入者検知装置側 ID 情報と、上記携帯端末側 ID 情報とが一致するか否かを示す情報に基づき生成される情報であって、上記物体がユーザであるか否かを示す移動物体識別情報に基づいて、上記威嚇実行手段に対して威嚇処理の実行命令を付与する制御手段とを備えることを特徴とする侵入者検知装置。

**【請求項 2】**

監視領域への不正侵入者を威嚇する威嚇処理を実行可能な外部の威嚇実行手段に対して威嚇処理の実行命令を付与する侵入者検知装置において、

自身が送波したマイクロ波が被検知物により反射されて生成される反射波における周波数の変化を測定することで、移動している物体の検知、および、ユーザを特定することが可能なユーザに固有の動作の検知を行うドップラーセンサーと、

上記ドップラーセンサーにより上記反射波における周波数の変化が測定されたか否かを示す情報に基づき生成される情報であって、移動している物体があるか否かを示す移動物体有無情報に基づき、上記ドップラーセンサーにより上記反射波における周波数の変化が測定されたか否かを示す情報に基づき生成される情報であって、ユーザに固有の動作を特定するための固有動作情報と、上記侵入者検知装置内に予め登録されたユーザを特定することが可能な侵入者検知装置側 ID 情報とを照合することによって、上記物体がユーザであるか否かを識別する認証処理手段と、

上記固有動作情報と、上記侵入者検知装置側 ID 情報とが一致するか否かを示す情報に基づき生成される情報であって、上記物体がユーザであるか否かを示す移動物体識別情報に基づいて、上記威嚇実行手段に対して威嚇処理の実行命令を付与する制御手段とを備えることを特徴とする侵入者検知装置。

**【請求項 3】**

監視領域への不正侵入者を威嚇する威嚇処理を実行する威嚇実行手段と、請求項 1 または 2 に記載の侵入者検知装置とを有することを特徴とする侵入者威嚇装置。

**【請求項 4】**

請求項 3 の侵入者威嚇装置が車両に搭載されていることを特徴とする車両用侵入者威嚇装置。

**【請求項 5】**

ユーザにより特定の動作が車両に加えられることによって、車両の周囲の物体と車両との間に生じる相対移動を、上記ドップラーセンサーを用いて検知することを特徴とする請求項 4 に記載の車両用侵入者威嚇装置。

【書類名】 明細書

【発明の名称】 侵入者検知装置、侵入者威嚇装置、および車両用侵入者威嚇装置

【技術分野】

【0001】

本発明は、車両、建物等への物体の接近を検知し、物体の接近に対してユーザの認証処理を行い、これらの結果に応じて、外部の威嚇処理実行手段に侵入者に対する威嚇処理を実行させる侵入者検知装置、および、それを備えた侵入者威嚇装置に関する。

【背景技術】

【0002】

近年、車両や建物に対する防犯装置への必要性が急速に高まっている。広く市販されているものとして、不正なドアのこじ開けや、車両の傾斜等の車両異常を検知する機能を備え、異常が発生した際にはサイレンで車両への侵入者を威嚇する車載式の防犯装置を挙げることができる。

【0003】

このような防犯装置において、ユーザが、侵入者検知装置の警戒状態の設定、解除、あるいは威嚇処理の実行等を行う方法として、自動方式および手動方式がある。

【0004】

手動方式では、ユーザは防犯対象物へ接近あるいは遠ざかる毎に、意識的に操作を行い、侵入者検知装置の警戒状態の設定あるいは解除を行う。

【0005】

これに対し、自動方式の侵入者検知および威嚇を採用する防犯装置では、ユーザは意識的に操作を行わなくても、ユーザが防犯対象物に接近した時には、自動的に侵入者検知装置の警戒状態の解除が行われ、ユーザが防犯対象物から遠ざかる時には、自動的に侵入者検知装置の警戒状態への移行の操作が行われる。

【0006】

例えば、侵入者検知装置と通信可能な携帯装置を持ったユーザが、車両等の防犯対象物に近づく際に、携帯装置と侵入者検知装置との通信によるID認証が行われ、ユーザが携帯装置のキースイッチを押すなどの意識的な操作を行うことなく、侵入者検知装置の警戒状態の解除が行われる。

【0007】

また、自動方式では、ユーザが車両等を離れる際において、エンジンを切ってから設定された時間が経過した後に、自動的に侵入者検知装置の警戒状態の設定が行われるといった方法も利用される。

【0008】

これらの従来の自動方式の侵入者検知装置において、ID認証を行うためのユーザを特定することが可能なID情報は、通常、ユーザが携帯する携帯装置（キーやリモコンなど）内と、侵入者検知装置内とに登録されており、認証処理手段により、侵入者検知装置内に登録されたID情報とユーザが携帯する携帯装置内に登録されたID情報とを照合させてID認証処理を行う。そのため、侵入者検知装置の警戒状態の解除を制御するデバイスからユーザの持つデバイスに通信し、微弱無線や小電力無線方式が用いられる。

【0009】

しかしながら、ID認証処理を常時行う場合は、常に無線通信を行うことになり、電力消費量が増大する。特に、バッテリーや電池など、電力を継続的に供給することのできない電源で作動することの多い車載方式の侵入者検知装置の場合は、電源を使用することが可能な時間が著しく低減されてしまう。

【0010】

逆に、バッテリーの耐久時間をなるべく長くするために、周期的にID認証を行うとともに、一旦ID認証処理が終ってから次のID認証処理が開始されるまでの時間間隔を長くした場合は、ID認証処理が行われていない時間を増やすことになり、ユーザ以外の者が不正に車両に近づく可能性が高まってしまう。これでは、侵入者検知装置の利便性が悪

くなくなってしまう。

【0 0 1 1】

そこで従来の侵入者検知装置においては、I D 認証処理を、ユーザが行う動作をきっかけに開始する方式が採用されている。例えば、接触センサーによりユーザがドアノブを触ったときの静電容量の変化を検知したり、ユーザの持つ携帯装置に設けられた振動センサーにより、ユーザが移動する際の携帯装置の振動を検知したりすることをきっかけに、I D 認証処理を開始する方式が採用されている。

【0 0 1 2】

その他、特許文献 1 において、電波式ドップラーセンサーにより、電波発射器から発射された電波の反射波を受信して人が接近することを検知する、車載式の防犯装置について述べられている。

【0 0 1 3】

また、特許文献 2 において、人間から発射される熱線を検知する焦電センサーと、焦電センサーによる検知結果に呼応して、自身より送波されたマイクロ波とその人間からの検出波との周期を解析し、その人間が侵入者であるかの判断を行うドップラーセンサーと、ドップラーセンサーによる判断結果に基づいて、その人間を侵入者であるとみなした場合にのみ、威嚇処理を実行する警報装置とを備える侵入者検知装置について述べられている。

【0 0 1 4】

さらに、正規の運転者が車両へ乗ったこと、もしくは正規の運転者が車両へ接近したことが検出されたとき、又は使用者により所定操作が行われたときに、車両盗難防止装置の盗難警戒モードが解除されるようにする技術を開示するものとして、特許文献 3 がある。

【0 0 1 5】

また、ドップラーセンサーにより車両に加えられた振動と車両への侵入者の動作とを、ドップラー信号の継続時間の差に着目して区別し、車両への進入者を検知した場合にのみ威嚇処理を実行する機能を有する車両盗難防止装置について開示している特許文献 4 がある。

【特許文献 1】 特開平 8 - 3 2 9 3 5 8 号公報（平成 8 年 1 2 月 1 3 日公開）

【特許文献 2】 特開 2 0 0 1 - 3 4 8 5 5 号公報（平成 1 3 年 2 月 9 日公開）

【特許文献 3】 特開 2 0 0 3 - 1 8 2 5 2 4 号公報（平成 1 5 年 7 月 3 日公開）

【特許文献 4】 特公平 7 - 5 0 6 2 号公報（昭和 6 1 年 8 月 2 日公開）

【発明の開示】

【発明が解決しようとする課題】

【0 0 1 6】

しかしながら、従来技術のように、ユーザがドアノブに接触することを検知して I D 認証を開始する方式においては、以下の問題点がある。すなわち、当該方式では、運転席に設けられたドア以外のドアにおけるドアノブを操作した場合にも、侵入者検知装置の警戒状態の解除を自動的に行えるようにするため、複数のドアにそれぞれ接触センサーを設ける必要がある。このように接触センサーを複数設けると、侵入者検知装置の大型化・高コスト化を招くという問題がある。

【0 0 1 7】

また、携帯装置に振動センサーを設置して、振動センサーによりユーザが移動する際の携帯装置の振動を検知することをきっかけに、I D 認証処理を開始する方式においては、ユーザが車両の近くにいない場合でも、I D 認証を開始する旨の要求が携帯装置から侵入者検知装置に送信される場合がある。しかしながら、携帯装置と侵入者検知装置とが無線通信可能なエリア外にユーザがいれば、そのような I D 認証の開始要求は侵入者検知装置には受信されない。よって、不必要な無線通信に伴う無駄な電力消費を抑制することができない。

【0 0 1 8】

また、特許文献 1 に記載の技術では、ドップラーセンサーにより送波したマイクロ波の

周期よりも検出波の周期が短い場合に、侵入する意志を有する者が監視エリアに近づいていると判断する。しかしながら、侵入する意志を有しない者が監視エリアに近づいている場合においても、マイクロ波の周期は検出波の周期よりも短くなるので、その者は侵入する意志があると判断されてしまう。したがって、特許文献1に記載の技術では、侵入する意志を有しない者が監視エリアに近づく場合においても警報装置が作動するので、侵入者のみに対する的確な警報を行っているとはいえない。

#### 【0019】

また、特許文献2に記載の技術では、警報器にタイマー回路を付設することにより、移動体が車両外部に居る時間に応じて段階的に警報を変化させる。したがって、車両の正規ユーザが車両外部に長く居るような状況、たとえば荷物の積み下ろしを行っている状況や洗車しているような状況においても大音量の警報が警報器により発せられる可能性がある。したがって、特許文献2に記載の技術も、特許文献1に記載の技術と同様に、侵入者のみに対する的確な警報を行っているとはいえない。

#### 【0020】

さらに、特許文献3に記載の技術では、車両盗難防止装置と携帯用発信器との間で通信を行うことにより、運転者が車両に接近したか否かを判断する。このような通信には電力を浪費する場合が多いので、特許文献3に記載の技術では、運転者が車両に接近することを検知するために無駄な電力が消費されてしまう。

#### 【0021】

また、特許文献4に記載の技術では、ドップラーセンサーにより正規のユーザが車両に進入することが検知された場合のドップラー信号、および同センサーにより窃盗を目的とする者が車両に進入することが検知された場合のドップラー信号のいずれにも、同様の継続時間の差が、車両に加えられた振動を検知するドップラー信号との間に生じる。したがって、正規ユーザが車両に進入した場合にも、警報装置が作動する場合がある。したがって、特許文献4に記載の技術も、侵入者のみに対する的確な警報を行っているとはいえない。

#### 【0022】

本発明では、上記の従来の問題に鑑みてなされたものであり、その目的は、装置の大型化・高コスト化・消費電力の増大を生じること無く、侵入者検知装置の警戒状態設定、解除、あるいは威嚇処理の実行を行うために必要なID認証を、十分かつ無駄無く行うことのできる侵入者検知装置、およびそれを備えた侵入者威嚇装置を実現することにある。

#### 【課題を解決するための手段】

#### 【0023】

本発明の侵入者検知装置は、上記課題を解決するために、監視領域への不正侵入者を威嚇する威嚇処理を実行可能な外部の威嚇実行手段に対して威嚇処理の実行命令を付与する侵入者検知装置において、自身が送波したマイクロ波が被検知物により反射されて生成される反射波における周波数の変化を測定することで、移動している物体を検知するドップラーセンサーと、自身の外部と通信可能な通信手段と、上記ドップラーセンサーにより上記反射波における周波数の変化が測定されたか否かを示す情報に基づき生成される情報であって、移動している物体があるか否かを示す移動物体有無情報に基づき、上記通信手段とユーザにより携帯される携帯端末との通信により、該携帯端末に予め登録されたユーザを特定することが可能な携帯端末側ID情報を読み出すとともに、上記侵入者検知装置内に予め登録されたユーザを特定することが可能な侵入者検知装置側ID情報と、上記携帯端末側ID情報とを照合することによって、上記物体がユーザであるか否かを識別する認証処理手段と、上記侵入者検知装置側ID情報と、上記携帯端末側ID情報とが一致するか否かを示す情報に基づき生成される情報であって、上記物体がユーザであるか否かを示す移動物体識別情報に基づいて、上記威嚇実行手段に対して威嚇処理の実行命令を付与する制御手段とを備えることを特徴とする。

#### 【0024】

上記構成によれば、マイクロ波を用いることで接近物を高感度で検知できるドップラー

センサーの検知に応答して識別処理を開始するため、侵入者検知の信頼性を向上することができる。

【0025】

また、認証処理手段においては、上記ドップラーセンサーにより上記反射波における周波数の変化が測定されたか否かを示す情報に基づき生成される、移動している物体があるか否かを示す移動物体有無情報に基づき、移動している物体がユーザであるか否かを識別する処理が行われる。したがって、車両への接近物がドップラーセンサーに検知された場合に、認証処理手段によるユーザの識別処理が開始されるようにできるため、不必要な識別処理に伴う無駄な電力消費を抑制することができる。

【0026】

さらに、制御手段は、上記侵入者検知装置側ID情報と、上記携帯端末側ID情報とが一致するか否かを示す情報に基づき生成される、上記物体がユーザであるか否かを示す移動物体識別情報に基づき、威嚇実行手段に威嚇実行処理の実行命令を付与するので、識別処理により車両への接近者が車両の正規ユーザでないと判断された場合にのみ、その者に対して威嚇処理を実行することができる。よって、車両への侵入者のみに対する的確な警報を行うことができる。

【0027】

さらに、ドップラーセンサーは、マイクロ波の送波方向を調整することにより、広い領域内の移動している物体を検知できるため、たとえば車両の一箇所に設置されるだけで、多方向からのユーザの車両への接近を検知することができる。すなわち、ドップラーセンサーを車両の複数の箇所に設置すること無く、ユーザが車両の周囲における特定の領域に居ない場合でも、認証処理手段により識別処理を開始するようにできる。よって、大型化・高コスト化を抑制することができる。

【0028】

さらに、認証処理手段は、侵入者検知装置側ID情報と、携帯端末側ID情報とを照合することによって、識別処理を行うので、より高精度の識別処理を行うことができる。よって、車両への侵入者のみに対する的確な威嚇処理を、よりの確に外部の威嚇処理実行手段に実行させることができる。

【0029】

以上を示した理由により、大型化、高コスト化、あるいは、使用コストの上昇を生じること無く、確実かつ無駄の無い侵入者検知を行うことができる侵入者検知装置を実現できる。

【0030】

また、本発明の侵入者検知装置は、上記課題を解決するために、監視領域への不正侵入者を威嚇する威嚇処理を実行可能な外部の威嚇実行手段に対して威嚇処理の実行命令を付与する侵入者検知装置において、自身が送波したマイクロ波が被検知物により反射されて生成される反射波における周波数の変化を測定することで、移動している物体の検知、および、ユーザを特定することが可能なユーザに固有の動作の検知を行うドップラーセンサーと、上記ドップラーセンサーにより上記反射波における周波数の変化が測定されたか否かを示す情報に基づき生成される情報であって、移動している物体があるか否かを示す移動物体有無情報に基づき、上記ドップラーセンサーの検知結果に基づき生成される、ユーザに固有の動作を特定するための固有動作情報と、上記侵入者検知装置内に予め登録されたユーザを特定することが可能な侵入者検知装置側ID情報とを照合することによって、上記物体がユーザであるか否かを識別する認証処理手段と、上記固有動作情報と、上記侵入者検知装置側ID情報とが一致するか否かを示す情報に基づき生成される情報であって、上記物体がユーザであるか否かを示す移動物体識別情報に基づいて、上記威嚇実行手段に対して威嚇処理の実行命令を付与する制御手段とを備えることを特徴としている。

【0031】

上記構成によれば、マイクロ波を用いることで接近物を高感度で検知できるドップラーセンサーの検知結果に応答して、認証処理手段による識別処理が開始されるため、侵入者

検知の信頼性を向上することができる。

【0032】

また、認証処理手段においては、ユーザに固有の動作を特定するための固有動作情報に基づき、識別処理が行われる。したがって、ユーザにより固有の動作が行われた場合に、認証処理手段によるユーザの識別処理が開始されるようにできるため、不必要な処理に伴う無駄な電力消費を抑制することができる。

【0033】

さらに、制御手段は、上記固有動作情報と、上記侵入者検知装置側ID情報とが一致するか否かを示す情報に基づき生成される情報であって、物体がユーザであるか否かを示す移動物体識別情報に基づいて、威嚇実行手段に威嚇実行処理の実行命令を付与するので、認証処理手段により正規ユーザの固有動作が行われていないと判断された場合にのみ、その者に対して威嚇処理を実行することができる。よって、車両への侵入者のみに対して的確な警報を行うことができる。

【0034】

さらに、ドップラーセンサーは、マイクロ波の送波方向を調整することにより、広い領域内の移動している物体を検知できるため、たとえば車両の一箇所に設置されるだけで、広い範囲でユーザの動作を検知することができる。すなわち、ドップラーセンサーを車両の複数の箇所に設置すること無く、ユーザが車両の周囲における特定の領域に居ない場合でも、認証処理手段により識別処理を開始するようにできる。よって、大型化・高コスト化を抑制することができる。

【0035】

以上を示した理由により、大型化、高コスト化、あるいは、使用コストの上昇を生じること無く、確実かつ無駄の無い侵入者検知を行うことができる侵入者検知装置を実現できる。

【0036】

また、ドップラーセンサーを用いてユーザに固有の動作を検知することで識別処理を行うので、ドップラーセンサーを、認証処理手段の一部として用いることができる。したがって、侵入者検知装置の構成を簡略化することができる。

【0037】

また、ユーザは、ID情報が記録された携帯端末を携帯していなくても、自己に固有の動作を実行することにより、認証処理手段に識別処理を実行させることができる。つまり、ユーザは、携帯端末を有していなくても、制御手段から威嚇処理実行手段に威嚇処理の実行命令が付与されないようにすることができるので、ユーザの利便性を高めることができる。

【0038】

また、本発明の侵入者威嚇装置は、上記課題を解決するため、監視領域への不正侵入者を威嚇する威嚇処理を実行する威嚇実行手段と、上記構成のいずれかの侵入者検知装置とを有することを特徴としている。

【0039】

上記の構成によれば、侵入者威嚇装置は、適切な侵入者検知を行う侵入者検知装置を用いて威嚇処理を実行することができるので、不必要な威嚇処理の実行を防止しながら、侵入者に対しては確実に威嚇処理を行うことができる。したがって、消費電力量を抑制しつつ、侵入者に対して的確な威嚇処理を実行することができる。

【0040】

本発明の車両用侵入者威嚇装置は、上記侵入者威嚇装置が車両に搭載されていることを特徴とする。

【0041】

上記の構成によれば、侵入者威嚇装置が車両に取り付けられることにより、最も盗難されることの多い車両について防犯対策を施すことができる。

【0042】

本発明の車両用侵入者威嚇装置は、上記課題を解決するために、ユーザにより特定の動作が車両に加えられることによって、車両の周囲の物体と車両との間に生じる相対移動を、上記ドップラーセンサーを用いて検知することを特徴としている。

#### 【0043】

上記の構成によれば、ユーザによる特定動作が車両に加えられた際に生じる相対移動をドップラーセンサーで検知し、その検知結果に基づき識別処理を開始する。したがって、識別処理を行うために携帯端末と侵入者検知装置との間における通信強度の強弱を観察する必要がなくなるので、不必要な通信を低減し、消費電力を抑制することができる。

#### 【発明の効果】

#### 【0044】

以上のように、本発明の侵入者検知装置は、監視領域への不正侵入者を威嚇する威嚇処理を実行可能な外部の威嚇実行手段に対して威嚇処理の実行命令を付与する侵入者検知装置において、自身が送波したマイクロ波が被検知物により反射されて生成される反射波における周波数の変化を測定することで、移動している物体を検知するドップラーセンサーと、自身の外部と通信可能な通信手段と、上記ドップラーセンサーにより上記反射波における周波数の変化が測定されたか否かを示す情報に基づき生成される情報であって、移動している物体があるか否かを示す移動物体有無情報に基づき、上記通信手段とユーザにより携帯される携帯端末との通信により、該携帯端末に予め登録されたユーザを特定することが可能な携帯端末側ID情報を読み出すとともに、上記侵入者検知装置内に予め登録されたユーザを特定することが可能な侵入者検知装置側ID情報と、上記携帯端末側ID情報とを照合することによって、上記物体がユーザであるか否かを識別する認証処理手段と、上記侵入者検知装置側ID情報と、上記携帯端末側ID情報とが一致するか否かを示す情報に基づき生成される情報であって、上記物体がユーザであるか否かを示す移動物体識別情報に基づいて、上記威嚇実行手段に対して威嚇処理の実行命令を付与する制御手段とを備えているものである。

#### 【0045】

上記構成によれば、マイクロ波を用いることで接近物を高感度で検知できるドップラーセンサーの検知に応答して識別処理を開始するため、侵入者検知の信頼性を向上することができる。

#### 【0046】

また、認証処理手段においては、上記ドップラーセンサーにより上記反射波における周波数の変化が測定されたか否かを示す情報に基づき生成される、移動している物体があるか否かを示す移動物体有無情報に基づき、移動している物体がユーザであるか否かを識別する処理が行われる。したがって、車両への接近物がドップラーセンサーに検知された場合に、認証処理手段によるユーザの識別処理が開始されるようにできるため、不必要な識別処理に伴う無駄な電力消費を抑制することができる。

#### 【0047】

さらに、制御手段は、上記侵入者検知装置側ID情報と、上記携帯端末側ID情報とが一致するか否かを示す情報に基づき生成される、上記物体がユーザであるか否かを示す移動物体識別情報に基づき、威嚇実行手段に威嚇実行処理の実行命令を付与するので、識別処理により車両への接近者が車両の正規ユーザでないと判断された場合にのみ、その者に対して威嚇処理を実行することができる。よって、車両への侵入者のみに対する的確な警報を行うことができる。

#### 【0048】

さらに、ドップラーセンサーは、マイクロ波の送波方向を調整することにより、広い領域内の移動している物体を検知できるため、たとえば車両の一箇所に設置されるだけで、多方向からのユーザの車両への接近を検知することができる。すなわち、ドップラーセンサーを車両の複数の箇所に設置すること無く、ユーザが車両の周囲における特定の領域に居ない場合でも、認証処理手段により識別処理を開始するようにできる。よって、大型化・高コスト化を抑制することができる。

## 【0049】

さらに、認証処理手段は、侵入者検知装置側 ID 情報と、携帯端末側 ID 情報とを照合することによって、識別処理を行うので、より高精度の識別処理を行うことができる。よって、車両への侵入者のみに対する的確な威嚇処理を、よりの確に外部の威嚇処理実行手段に実行させることができる。

## 【0050】

以上に示した理由により、大型化、高コスト化、あるいは、使用コストの上昇を生じること無く、確実かつ無駄の無い侵入者検知を行うことができる侵入者検知装置を実現できる。

## 【0051】

また、本発明の侵入者検知装置は、以上のように、監視領域への不正侵入者を威嚇する威嚇処理を実行可能な外部の威嚇実行手段に対して威嚇処理の実行命令を付与する侵入者検知装置において、自身が送波したマイクロ波が被検知物により反射されて生成される反射波における周波数の変化を測定することで、移動している物体の検知、および、ユーザを特定することが可能なユーザに固有の動作の検知を行うドップラーセンサーと、上記ドップラーセンサーにより上記反射波における周波数の変化が測定されたか否かを示す情報に基づき生成される情報であって、移動している物体があるか否かを示す移動物体有無情報に基づき、上記ドップラーセンサーの検知結果に基づき生成される、ユーザに固有の動作を特定するための固有動作情報と、上記侵入者検知装置内に予め登録されたユーザを特定することが可能な侵入者検知装置側 ID 情報とを照合することによって、上記物体がユーザであるか否かを識別する認証処理手段と、上記固有動作情報と、上記侵入者検知装置側 ID 情報とが一致するか否かを示す情報に基づき生成される情報であって、上記物体がユーザであるか否かを示す移動物体識別情報に基づいて、上記威嚇実行手段に対して威嚇処理の実行命令を付与する制御手段とを備えているものである。

## 【0052】

上記構成によれば、マイクロ波を用いることで接近物を高感度で検知できるドップラーセンサーの検知結果に応答して、認証処理手段による識別処理が開始されるため、侵入者検知の信頼性を向上することができる。

## 【0053】

また、認証処理手段においては、ユーザに固有の動作を特定するための固有動作情報に基づき、識別処理が行われる。したがって、ユーザにより固有の動作が行われた場合に、認証処理手段によるユーザの識別処理が開始されるようにできるため、不必要な処理に伴う無駄な電力消費を抑制することができる。

## 【0054】

さらに、制御手段は、上記固有動作情報と、上記侵入者検知装置側 ID 情報とが一致するか否かを示す情報に基づき生成される情報であって、物体がユーザであるか否かを示す移動物体識別情報に基づいて、威嚇実行手段に威嚇実行処理の実行命令を付与するので、認証処理手段により正規ユーザの固有動作が行われていないと判断された場合にのみ、その者に対して威嚇処理を実行することができる。よって、車両への侵入者のみに対して的確な警報を行うことができる。

## 【0055】

さらに、ドップラーセンサーは、マイクロ波の送波方向を調整することにより、広い領域内の移動している物体を検知できるため、たとえば車両の一箇所に設置されるだけで、広い範囲でユーザの動作を検知することができる。すなわち、ドップラーセンサーを車両の複数の箇所に設置すること無く、ユーザが車両の周囲における特定の領域に居ない場合でも、認証処理手段により識別処理を開始するようにできる。よって、大型化・高コスト化を抑制することができる。

## 【0056】

以上に示した理由により、大型化、高コスト化、あるいは、使用コストの上昇を生じること無く、確実かつ無駄の無い侵入者検知を行うことができる侵入者検知装置を実現でき

る。

【0057】

また、ドップラーセンサーを用いてユーザに固有の動作を検知することで識別処理を行うので、ドップラーセンサーを、認証処理手段の一部として用いることができる。したがって、侵入者検知装置の構成を簡略化することができる。

【0058】

また、ユーザは、ID情報が記録された携帯端末を携帯していなくても、自己に固有の動作を実行することにより、認証処理手段に識別処理を実行させることができる。つまり、ユーザは、携帯端末を有していなくても、制御手段から威嚇処理実行手段に威嚇処理の実行命令が付与されないようにすることができるので、ユーザの利便性を高めることができる。

【発明を実施するための最良の形態】

【0059】

本発明の実施形態について、図1ないし図6に基づいて説明すると以下の通りである。なお、本実施形態は、本発明の侵入者検知装置を車載式の防犯装置に適用した場合について記載したものである。

【0060】

本実施形態の侵入者検知装置1は、図1に示すように、マイクロ波を送波し対象物からの反射波の周波数やエネルギー等の変化を測定することで、移動している物体を検知することができるドップラーセンサー2と、ユーザの携帯するリモコン等の携帯端末7と無線通信を行い、携帯端末側ID情報を読み出すことが可能である通信部5と、侵入者検知装置側ID情報が登録された記録部6と、携帯端末側ID情報および侵入者検知装置側ID情報を照合させることで上記移動している物体がユーザであるか否かを識別する認証処理部（認証処理手段）3と、侵入者検知装置1の後述する待機状態の設定・解除、後述する警戒状態の設定・解除、および威嚇処理の実行命令を行う制御部（制御装置）4とから構成される。なお、記録部6は通信部5内に備えられている。

【0061】

なお、特許請求の範囲および本明細書において、携帯端末側ID情報とは携帯端末7側に登録されたユーザを特定することが可能な固有の情報のことであり、侵入者検知装置側ID情報とは侵入者検知装置1側に登録されたユーザを特定することが可能な固有の情報のことである。

【0062】

また、ドップラーセンサー2は物体の接近を検知すると、制御部4へ移動物体有無情報を送信する。そして、制御部4は移動物体有無情報を受信すると、その解析を行い、その解析結果に基づいて、移動している物体がユーザであるか否かを識別する処理を行うよう認証処理部3へ命令を出す。なお、移動物体有無情報とは、ドップラーセンサーの検知結果に基づき生成される、移動している物体があるか否かを示す情報のことである。

【0063】

また、認証処理部3は、移動している物体がユーザであるか否かを識別する処理を行うと、制御部4へ移動物体識別情報を送り、制御部4は、移動物体有無情報を受信すると、その移動物体識別情報に基づいて、後述する外部の威嚇実行部10へ威嚇処理の実行命令を出す。なお、移動物体識別情報とは、認証処理部3の識別結果に基づき生成される、接近物がユーザであるか否かを示す情報のことである。

【0064】

また、侵入者検知装置1は、車両が走行している間にシガーアダプターから電力を供給される充電電池を電源として用いる。一方、携帯端末7は、電源として侵入者検知装置1の電源とは別に電池を用い、外部から電力を供給されることなく、数日間連続して使用されることが可能である。

【0065】

さらに、侵入者検知装置1の外部には侵入者検知装置1に接続された威嚇実行部（威嚇

実行手段) 10が備えられており、制御部4による威嚇処理を実行する命令に応じて、侵入者に対して威嚇処理を行う。なお、「威嚇処理」としては、後述するようにブザーの鳴動、LEDの発光動作を用いることができる。

#### 【0066】

また、侵入者検知装置1と威嚇実行部10とを一体的に構成したユニットを、本明細書および特許請求の範囲においては「侵入者威嚇装置」として記載している。

#### 【0067】

また、威嚇実行部10としてはLEDやブザーを使用することができる。LEDやブザーは、ユーザ以外の接近する物体に対する威嚇処理だけでなく、動作確認のためにも使用される。LEDは、動作確認の際は発光強度の弱い、あるいは周期の長い点滅を行い、威嚇処理の際は発光強度の強い、あるいは周期の短い点滅を行うように設定される。LEDやブザーを用いて、ユーザでない接近する物体に対して威嚇処理を行う際、周囲の人間に対しての異常発生を知らせる効果も得ることができる。

#### 【0068】

なお、本明細書および特許請求の範囲において、侵入者検知装置1の警戒状態とは、ドップラーセンサー2により侵入者検知装置1の周囲で移動する物体を検知することができ、通信部5により携帯端末7と通信可能であり、認証処理手段による認証処理が可能であり、制御部4の命令に応じて、威嚇実行部10により威嚇処理を実行することが可能な状態を意味する。一方、侵入者検知装置1の待機状態とは、制御部4により、侵入者検知装置1の動作していない状態が終了した時点から、侵入者検知装置1の警戒状態が開始する時点までの状態、あるいは、再び侵入者検知装置1の動作していない状態が開始する時点までの状態である。この待機状態において、威嚇実行部10による威嚇処理は実行されない。

#### 【0069】

また、携帯端末7は、携帯端末側ID情報が登録された記録部8を備え、ID認証のために使用されるだけでなく、ユーザが手動で侵入者検知装置1の警戒状態の設定・解除を行うためにも使用される。ユーザによる手動での侵入者検知装置1の警戒状態の設定・解除は、ユーザが携帯端末7に備えられた侵入者検知装置1の警戒状態の設定・解除ボタンを押すと、その旨は通信部5と携帯端末7との無線通信により侵入者検知装置1へ送信され、それに応答して制御部4により侵入者検知装置1の警戒状態の設定・解除を行う方法を用いて行われる。

#### 【0070】

まず、図2および図3を用いて、ユーザが車両を利用しない場合に、侵入者検知装置1の警戒状態の設定を行う手順について説明する。図2は、自動警戒設定の手順を説明するための図である。また、図3は、自動警戒設定の手順を示したフローチャート図である。なお、自動警戒設定とは、ユーザが意識的な操作を行うことなく、自動的に侵入者検知装置1の警戒状態の設定が行われることを意味する。

#### 【0071】

なお、侵入者検知装置1が取り付けられている車両をユーザが運転している際は、侵入者検知装置1は作動しない状態となっており、一方、ユーザが車両を離れる際、侵入者検知装置1は、自動警戒設定が可能な状態となっている。

#### 【0072】

図2に示すように、ユーザが車両のエンジンをオフした場合に、侵入者検知装置1への電源供給が停止することをトリガーにして、侵入者検知装置1は、自動的に待機状態に移行する。

#### 【0073】

待機状態において、通信部5(図1参照)はユーザの持つ携帯端末7と無線通信を行う。そして、制御部4(図1参照)は、通信部5(図1参照)と携帯端末7との間における通信感度から携帯端末7と車体との距離を測定する、距離測定処理を開始する。

#### 【0074】

そして、図 2 に示すように、ユーザが携帯端末 7 を持った状態で車両を離れていくとする。この過程において、距離測定処理により、ユーザが車体から近いと判断された場合は、待機状態が継続される。そして、距離測定により、ユーザが車両を離れた、すなわちユーザが車両から遠いと判断された場合、自動的に制御部 4 により侵入者検知装置 1 の警戒状態の設定が行われる。

#### 【0 0 7 5】

図 3 を用いて、自動警戒設定がなされる手順についてさらに詳細に説明する。ユーザが車両のエンジンをオフした場合（S 1）、車両から侵入者検知装置 1 への電源供給が停止され、侵入者検知装置 1 は自身の充電電池を電源として用いて動作するようになる。自動警戒設定が ON となっていれば（S 2）、車両からの電源供給の停止をトリガーにして、侵入者検知装置 1 は自動的に待機状態に移行する（S 3）。

#### 【0 0 7 6】

待機状態では、通信部 5 はユーザの持つ携帯端末 7 と無線通信を行い、制御部 4 は通信部 5 と携帯端末 7 との通信感度から、携帯端末 7 と車体との距離を測定する（S 4、S 5）。

#### 【0 0 7 7】

S 4 における距離測定は予め設定された時間間隔、例えば 1 0 秒間隔で行われ、これにより、ユーザが予め設定された車体からの距離内、例えば車両から 5 m 以内にいると判断された場合は、制御部 4 により予め設定された時間、例えば 1 0 分の間だけ待機状態が継続される（S 6）。すなわち、制御部 4 により、現在の状況が、エンジンオフ後ユーザが乗降中であつたり、荷物の積み下ろしを行っていたりする状況であると判断される。

#### 【0 0 7 8】

距離測定により、ユーザは予め設定された車体からの距離外にいると判定された場合、すなわち、ユーザは車両を離れたと判断された場合、自動的に、制御部 4 により侵入者検知装置 1 の警戒状態の設定が行われる（S 8）。このため、ユーザは警戒状態を設定するための意識的な操作、例えば携帯端末 7 における警戒状態設定スイッチを押すなどの操作を行う必要が無い。また、自動的に警戒状態が設定された場合は、その旨が通信部 5 により携帯端末 7 に通知され、この通知に基づき、携帯端末 7 から警戒状態が設定された旨の音声メッセージが発せられたり、携帯端末 7 における画像表示部に警戒状態が設定された旨が表示される。これにより、ユーザは自動的に警戒状態が設定されたことを確認できるようになっている。

#### 【0 0 7 9】

S 6 において待機状態が継続された後、待機状態がエンジンオフ後に予め設定された時間継続してタイムアウトしたか否かが、制御部 4 により判断される（S 7）。S 7 においてタイムアウトしていないと判断された場合、S 4 に戻り距離測定処理が継続される。一方、S 7 においてタイムアウトしたと判断された場合、すなわち、ユーザが車両のエンジンオフ後に設定された時間を超過しても車両から遠ざからない場合、制御部 4 により待機状態は解除され、侵入者検知装置 1 の作動しない状態へ移行する。侵入者検知装置 1 が作動しない状態へ移行したことは、通信部 5 により携帯端末 7 に通知され、ユーザは確認することができる。

#### 【0 0 8 0】

なお、本明細書における「侵入者検知装置 1 が作動しない状態」とは、侵入者検知装置 1 における各ブロックの全てが機能しない状態を意味するものではない。すなわち、上述の携帯端末 7 への通知処理を行うべく、侵入者検知装置 1 における制御部 4 および通信部 5 は作動している必要がある。

#### 【0 0 8 1】

このように通信部 5 により侵入者検知装置 1 の作動状況を携帯端末 7 に通知することにより、車両は利用しないがユーザが車両近くに居続ける場合などにおいて、ユーザは携帯端末 7 を用いて、手動で侵入者検知装置 1 の警戒状態の設定を行うことができる。もちろん、制御部 4 を用いて距離測定を行うことにより、ユーザが車両を離れたと判断される場

合においては、制御部 4 により自動的に警戒状態の設定が行われるようにしてもよい。

#### 【0082】

次に、ユーザが車両に接近する場合に、ユーザにおいて意識的な操作が行われることなく自動的に侵入者検知装置 1 の警戒状態の解除を行う手順について説明する。なお、車両が使用されていない場合、ドップラーセンサー 2 は、車両の周囲に近づく人物の接近を検知するため、作動している。ドップラーセンサー 2 は車両の周囲に近づく人物の接近を検知するために作動しているが、未だ車両の周囲に近づく人物を検知していない状態を、警戒状態の初期状態とする。

#### 【0083】

図 4 に示すように、警戒状態の初期状態において、ユーザが車両に近づくことにより、携帯端末 7 が徐々に車両に近づく状況を想定する。この際、ドップラーセンサー 2 は物体の接近を検知すると、図 1 に示すように、制御部 4 に移動物体有無情報を送る。制御部 4 は、移動物体有無情報を受信すると、認証処理部 3 へ、移動している物体がユーザであるか否かを識別する処理を行うよう命令し、それに応じて認証処理部 3 は ID 認証を開始する。

#### 【0084】

その後、図 4 に示すように、侵入者検知装置 1 は、携帯端末 7 と通信部 5（図 1 参照）との無線通信により携帯端末側 ID 情報を受信する。そして、認証処理部 3（図 1 参照）は、侵入者検知装置 1 内の記録部 6（図 1 参照）に登録された侵入者検知装置側 ID 情報を読み出し、携帯端末側 ID 情報と侵入者検知装置側 ID 情報とを照合することにより、ID 認証を行う。

#### 【0085】

そして、図 1 に示すように、認証処理部 3 により、上記二つの ID 情報が一致し、ID 認証が適合すると判断されれば、ID 認証が適合するという移動物体識別情報が制御部 4 へ送られる。この移動物体識別情報に基づいて、制御部 4 は侵入者検知装置 1 の警戒状態を解除する。上記二つの ID 情報が不一致であり、ID 認証が不適合であると判断されれば、ID 認証が不適合であるという移動物体識別情報が制御部 4 へ送られる。この移動物体識別情報に基づいて、制御部 4 は威嚇実行部 10 へ威嚇処理を実行するよう命令し、その命令に応じて威嚇実行部 10 は威嚇処理を実行する。

#### 【0086】

図 5 を用いて、自動警戒状態を解除する手順について、更に詳細に説明する。警戒状態の初期状態において、ドップラーセンサー 2 は、ユーザの接近を検知すると（S10）、移動物体有無情報を制御部 4 へ送信する。移動物体有無情報を受信すると、制御部 4 はドップラーセンサー 2 による検知結果の解析を行う（S11）。

#### 【0087】

検知結果の解析においては、まず、接近物が人であるかどうかの判断が行われる（S12）。接近物が人であるかどうかの判断は、例えば、接近物の下端位置、大きさ、あるいは、移動速度等を解析する方法により行われる。これらの値が人に該当する範囲にあると判断されれば、接近物は人であるとみなされる。

#### 【0088】

接近物が人であると制御部 4 に判断された場合は、続いて、制御部 4 により自動警戒作動範囲内で人が検知されたかどうかの判断が行われる（S13）。なお、本明細書および特許請求の範囲において、自動警戒作動範囲とは、予め設定された車体からの距離、例えば車両から 3 m であり、侵入者がその範囲内に居た場合に、威嚇実行部 10 により威嚇処理が行われる対象となる範囲である。また、S13 における判断は、制御部 4 が上述の距離測定処理を行うことにより実現されている。

#### 【0089】

制御部 4 が自動警戒作動範囲内での検知であると判断すれば、以下に示す ID 認証処理が行われる状態へ移行する（S14～S17）。ここで、人の接近でないと判断した場合、および、自動警戒作動範囲外での検知であると判断した場合は、侵入者検知装置 1 は警

戒状態の初期状態に戻る。

【0090】

ID認証処理は、通信部5がユーザの携帯する携帯端末7と無線通信し、認証処理部3が通信結果を解析することにより行われる。

【0091】

まず、制御部4は認証処理部3へID確認命令を出し(S14)、ID確認命令に応じて、認証処理部3は通信部5から携帯端末7への無線通信を通じて、携帯端末7へID情報を送信するように信号を送る。携帯端末7の種類が侵入者検知装置1と適合する場合は、携帯端末7はこの信号に反応して携帯端末側ID情報を通信部5へ送信する。ここで、まず、認証処理部3により携帯端末側ID情報を受信したか否かが判断される(S15)。

【0092】

認証処理部3により携帯端末7が侵入者検知装置1と適合すると判断された場合、すなわち、S15において通信部5が携帯端末側ID情報を受信した場合は、認証処理部3により侵入者検知装置側ID情報を読み出し、侵入者検知装置側ID情報と携帯端末側ID情報とを照合する(S16)。

【0093】

認証処理部3により、携帯端末側ID情報と侵入者検知装置側ID情報とは一致する、すなわちID認証は適合すると判断されれば、認証処理部3から制御部4へID認証は適合するという移動物体識別情報が送られる。この移動物体識別情報に応じて、制御部4は威嚇実行部10へ威嚇処理を実行するよう命令し、その命令に応じて、威嚇実行部10は、警戒状態を解除する(S17)。

【0094】

しかし、携帯端末7から携帯端末側ID情報が受信されない場合(S15でNoの場合)、および、認証処理部3により携帯端末側ID情報と侵入者検知装置側ID情報とが不一致、すなわちID認証が不適合であると判断された場合(S16で不適合の場合)は、認証処理部3から制御部4へID認証が不適合であるという移動物体識別情報が送られる。この移動物体識別情報に応じて、制御部4は威嚇実行部10へ威嚇処理を実行するよう命令し、その命令に応じて、威嚇実行部10は威嚇処理を実行する(S18)。

【0095】

ただし、接近者がユーザではなく、ID認証の結果として不適合の結果が得られた場合であっても、その接近者が故意に接近している侵入者ではない場合もあるので接近者に対する威嚇処理を段階的に行うことが好ましい。

【0096】

すなわち、最初の威嚇処理は接近者に注意を促す程度の短時間のブザー鳴動やLEDの点灯など軽い反応とし、ID認証処理が行われてから接近者が車両から遠ざかるまでの時間が、予め設定された時間、例えば10分を超過すると、第二の威嚇処理として長時間で大音量のブザー鳴動など大きな反応を行うようにすることが好ましい。

【0097】

さらに、ドップラーセンサー2により送波されるマイクロ波は、反射する物体の面積(速度)に応じてその反射波のエネルギーや周波数が変化する。例えば、車両への接近物が猫や鳥などの小動物の場合、人であった場合と比較して、マイクロ波が反射する面積が小さいため、反射波のエネルギーが小さくなるか、反射波が検出される時間が短くなる。また、車両への接近物が自転車などの人より速度の大きいものであった場合、反射波のエネルギー変化量は大きくなる。すなわち、ドップラーセンサー2により検知結果を解析することで、車両への接近物の大きさ(速度)を判別することができる。このことを利用し、ドップラーセンサー2による検知結果の解析により、接近物の大きさ(速度)が予め設定された範囲内にあると判断された場合にのみ、接近物を威嚇処理が実行される対象物として判断するようにしてもよい。

【0098】

例えば、小動物や車両など人以外の接近物については威嚇処理が実行されないように、制御部 4 により威嚇処理が実行される対象物と判断される接近物の大きさについて、高さが 1 m 以上であることが好ましく、また、高さが 1 ~ 2 m、かつ幅が 50 cm 以内であることがより好ましい。また、通過する自動車や電車には威嚇処理が実行されないように、制御部 4 により威嚇処理が実行される対象物と判断される接近物の速度は、5 m/秒であることが好ましく、1.5 ~ 3 m/秒であることがより好ましい。

#### 【0099】

ただし、人より大きい、あるいは、人より速度が大きいと判断される接近物を検知した場合は、接近物により車両に対して危害が加えられる可能性があるため、接近物に対して ID 認証は行わず、威嚇処理のみが行われるようにすることが好ましい。

#### 【0100】

また、ドップラーセンサー 2 が送波するマイクロ波の指向性を調整して、特定の方向からの物体の接近のみを検知するように設定することができる。すなわち、車両の全方向ではなく、例えば運転席のドアの横方向のみからの物体の接近を検知するように設定することも可能である。

#### 【0101】

これらの設定により、車両に接近する物の内、人間だけに威嚇処理を実行することができるため、あるいは、車両の全方向ではなく、侵入者が接近することの多い方向のみの領域について、ドップラーセンサー 2 が検知するようにするため、接近物の ID 認証のための通信を必要な場合にのみ行うようにすることができる。よって、無駄な通信を抑制し消費電力量を低減することができる。

#### 【0102】

上記のような方法により、侵入者検知装置 1 は、マイクロ波を用いることにより接近物を高感度で検知できるドップラーセンサー 2 の検知に応答して ID 認証を開始し、その結果に応じて侵入者検知装置 1 の警戒状態設定、解除、あるいは威嚇処理が実行されるため、侵入者のみに対して的確に威嚇処理を実行することができる。

#### 【0103】

また、上記のような方法により、人が車両に接近した際にのみ、認証処理部 3 により ID 認証処理を開始するため、ユーザあるいはユーザ以外の人が車両の近くにいない場合に無線通信を行う可能性が無い。よって、不必要な無線通信に伴う無駄な電力消費を抑制することができる。

#### 【0104】

さらに、ドップラーセンサー 2 は、マイクロ波の送波方向を調整することにより、広い領域の接近物を検知できるため、車両の一箇所に設置されるだけで、多方向からのユーザあるいはユーザ以外の人々の車両への接近を検知することができる。すなわち、ドップラーセンサー 2 を車両の複数の箇所に設置すること無く、ユーザあるいはユーザ以外の人々が車両の周囲の特定の領域に居ない場合でも、認証処理部 3 により ID 認証処理を開始することができる。よって、侵入者検知装置 1 の大型化・高コスト化を抑制することができる。

#### 【0105】

また、振動センサーにより振動を検知して ID 認証を開始する場合は、ユーザの携帯するリモコンなどの機器に振動センサーを組み込む必要があるが、リモコンはユーザにより携帯されて使用されるため、リモコンの中にセンサーを組み込む等の加工を行った場合に生じる大型化は好ましくない。これに対して、上記のような方法の場合は、ドップラーセンサー 2 は侵入者検知装置 1 の中に組み込まれており、ユーザは侵入者検知装置 1 を車両に設置して使用する。よって、携帯端末 7 を加工する必要が無く、それに伴う携帯端末 7 の大型化を抑制し、ユーザの使用環境の悪化を抑制することができる。

#### 【0106】

以上を示した理由により、上記の方法においては、侵入者検知装置 1 の大型化、高コスト化、あるいは、使用コストの上昇を生じること無く、確実かつ無駄の無い侵入者検知を行うことができるという効果を奏する。

**【0107】**

また、認証処理を開始するためだけでなく、認証処理を行うためにも、ドップラーセンサー2を利用することが可能である。ドップラーセンサー2が認証処理を行うために利用される場合、警戒状態の解除はユーザの意識的な操作により行われる手動方式の侵入者検知装置である。ユーザが車両を利用しない場合に、警戒状態の設定を行う手順については、上記に示したものと同様であり、上記の説明に従う。

**【0108】**

ドップラーセンサー2が認証処理を行うために用いられる場合の、警戒状態の解除の手順について図6を用いて説明する。図6は、ユーザにより意識的に操作を行うことで、侵入者検知装置1の警戒状態の解除を行う、手動方法の手順を示したフローチャート図である。

**【0109】**

車両が使用されていない場合、侵入者検知装置1は警戒状態に設定されている。警戒状態の初期状態において、ドップラーセンサー2はユーザの接近を検知すると（S20）、制御部4へ移動物体有無情報を送る。移動物体有無情報を受信すると、制御部4はドップラーセンサー2による検知結果の解析を行い（S21）、物体の接近が人であるかどうかの判断を行う（S22）。人であると判断された場合は、制御部4は、予め設定された自動警戒作動範囲内で物体が検知されたかどうかの判断を行う（S23）。

**【0110】**

自動警戒作動範囲内で物体が検知されたと判断されれば、制御部4から威嚇実行部10へ第一の威嚇処理を実行するように命令が発令され、それに応じて、威嚇実行部10により後述する第一の威嚇処理が行われる（S24）。

**【0111】**

また、第一の威嚇処理が行われると同時に、以下に示すID認証処理が行われる状態へ移行する（S25～S28）。制御部4により、接近物が人でないと判断された場合、および、自動警戒作動範囲外で検知されたと判断された場合は、警戒状態の初期状態に戻る。

**【0112】**

S25においては、ユーザによりID動作（ドップラーセンサー2を用いて認識されるユーザに固有の動作）が行われる。その後、ドップラーセンサー2により、ユーザによるID動作が検知されたか否かが判断される（S26）。なお、ID動作としては、たとえば、運転席ドアの中央付近で手を3秒以上振り続ける動作、車体や窓をノックしたり、タイヤを足で蹴ったりする動作を用いることができる。

**【0113】**

S26の処理でユーザのID動作がドップラーセンサー2により検知された場合、認証処理部3は、侵入者検知装置側ID情報を読み出し、ドップラーセンサー2の検知結果に基づき生成される、ユーザに固有の動作を特定するための固有動作情報と、侵入者検知装置側ID情報とを照合することによってID認証を行い（S27）、接近する物体がユーザであるかどうかの判断を行う（S28）。

**【0114】**

侵入者検知装置側ID情報と、固有動作情報とが一致し、認証処理部3により接近者はユーザであると判断されれば、認証処理部3は制御部4へ接近者はユーザであるという移動物体識別情報を送る。移動物体識別情報を受信すると、制御部4は威嚇実行部10へ第一の威嚇処理の停止命令を付与し、これに応じて威嚇実行部10は第一の威嚇処理を停止させる（S29）。また、制御部4により侵入者検知装置1は動作していない状態へ移行する。

**【0115】**

しかし、第一の威嚇処理開始後、予め設定された時間、例えば10分内に、ドップラーセンサー2によりID動作が検知されない場合（S26でNoの判断がなされた場合）、あるいは、侵入者検知装置側ID情報と、固有動作情報とが一致しない場合（S28で不

適合の判断がなされた場合)は、制御部 4 により接近者がユーザではないと判断され、後述する第二の威嚇処理が実行される (S 3 0)。

【0 1 1 6】

なお、威嚇処理は、上記フローのように、第一の威嚇処理を行った後に第二の威嚇処理を行うというように、段階的に行われることが好ましい。なぜなら、第一の威嚇処理は、接近者について、侵入者であるかユーザであるかの確認を行うための I D 認証を行っていない状態で実行されるためである。また、第二の威嚇処理は、接近者について I D 認証を行い、接近者をユーザでないと判断した場合に実行されるが、この場合も接近者は故意に接近している侵入者ではない場合があるからである。

【0 1 1 7】

よって、第一の威嚇処理として、物体の接近に注意を促す程度の短時間で小音量のブザー鳴動や L E D の点灯など軽い反応を行うようにし、I D 認証処理が行われた直後に、第二の威嚇処理として第一の威嚇処理より大音量あるいは長時間のブザー鳴動などの反応を行うようにし、さらに、I D 認証処理が行われてから接近者が車両から遠ざかるまでの時間が、予め設定された時間、例えば 1 0 分を超過すると、第三の威嚇処理としてさらに長時間で大音量のブザー鳴動など大きな反応を行うようにすることが好ましい。

【0 1 1 8】

この場合の I D 動作としては、例えば運転席ドアの中央付近で手を 3 秒以上振り続けることなどを用いることができる。

【0 1 1 9】

また、ドップラーセンサー 2 を高感度に調整すれば、車両自体の振動を検知できる。これは、ドップラーセンサー 2 が取り付けられた車両が揺れることにより、ドップラーセンサー 2 と周囲の物体の相対的位置関係が変化し、ドップラーセンサー 2 の周囲の物体が移動しているように検知されるためである。この事を利用して、例えば車体や窓をロックしたり、タイヤを足で蹴ったりすることにより車両に振動を起こし、ロックの間隔や回数による振動を特定するための情報を侵入者検知装置側 I D 情報として記録部 6 に登録することも可能である。

【0 1 2 0】

ここで、ドップラーセンサー 2 に検知される I D 動作を用いる場合、携帯端末 7 に登録される携帯端末側 I D 情報を用いる場合のように、高度なセキュリティを実現する必要がある。そこで、複数の動作を組み合わせることにより得られる一つの I D 動作を、ドップラーセンサー 2 に検知させるようにすることが好ましい。例えば、運転席付近で手を振ることと助手席付近で手を振ることを組み合わせると一つの I D 動作として用いることができる。

【0 1 2 1】

また、I D 認証を段階的に行うことが好ましい。例えば、第一段階の I D 認証の際に I D 動作を用い、第二段階の I D 認証の際に携帯端末 7 に登録された携帯端末側 I D 情報を用いることができる。

【0 1 2 2】

また、携帯端末 7 に登録された携帯端末側 I D 情報と、ドップラーセンサー 2 に検知される I D 動作とを合わせて利用することで、I D 認証の際に携帯端末 7 を忘れた場合の代替手段として、ドップラーセンサー 2 に検知される I D 動作を用いるようにしてもよい。

【0 1 2 3】

このようにユーザを特定するための固有情報として、ドップラーセンサー 2 により検知されたユーザの動作を示す情報を I D 認証処理に用いることで、上記に示したような I D 認証処理のための携帯端末 7 と通信部 5 との無線通信を行う必要がなくなり、さらに消費電力量を抑制することができる。

【0 1 2 4】

さらに、ドップラーセンサー 2 を高感度に調整することにより、車両自体の振動の検知が可能なことを利用して、車両の振動を I D 認証のトリガーとして利用することもできる

。例えば、車体に対して、窓を叩いたり足で蹴ったりする際に生じる振動が加えられた場合、ドップラーセンサー 2 により車両に振動が生じたことを検知する。その検知結果を示す情報に応答して制御部 4 から認証処理部 3 へ ID 認証の実行命令が出され、認証処理部 3 により ID 認証を開始するようにしてもよい。

#### 【0125】

このようにドップラーセンサー 2 により、車両自体の振動を検知するとともに、その検知結果を ID 認証のトリガーとして利用することによって、以下の利点を得ることができる。

#### 【0126】

すなわち、図 5 および図 6 に示したフローにおいて、ID 認証が行われるためのトリガーの 1 つを得るために、制御部 4 により、自動警戒作動範囲内で人が検知されたか否かの判断が行われている。この制御部 4 による判断は、通信部 5 と携帯端末 7 との通信感度からユーザと車体との距離を測定する、距離測定処理によって実現されている。

#### 【0127】

ここで、上述したようにドップラーセンサー 2 による車両振動の検知結果を ID 認証のトリガーとして利用すれば、制御部 4 による距離測定処理を行うことなく、ID 認証を開始させることができる。

#### 【0128】

また、ID 認証のトリガーとして用いられる、例えばタイヤを蹴る、車体や窓ガラスをたたくなどの行為は、通常の駐車状態では発生しにくいいため、ID 認証をより確実に無駄なく行うことができる。したがって、通信部 5 と携帯端末 7 との間における通信時間を低減し、さらに消費電力量を抑制することができる。

#### 【0129】

そして、ID 認証の結果、認証処理部 3 により、振動を起こしている者がユーザであると判断された場合は警戒状態の解除を行い、振動を起こしている者がユーザでないと判断された場合は威嚇処理を実行する。

#### 【0130】

この場合、ID 認証処理は、通信部 5 により携帯端末 7 内に登録された携帯端末側 ID 情報を受信し、その一方で、認証処理部 3 により侵入者検知装置側 ID 情報を読み出し、携帯端末側 ID 情報と侵入者検知装置側 ID 情報とを照合することによって、行われることが好ましい。また、ID 認証処理は、ドップラーセンサー 2 によりユーザの行う ID 動作を検知する一方、認証処理部 3 により侵入者検知装置側 ID 情報を読み出し、ユーザの行う ID 動作を示す固有動作情報と侵入者検知装置側 ID 情報とを照合することによって、行われることが好ましい。

#### 【0131】

ここで、ドップラーセンサー 2 が送波するマイクロ波は、ガラスやプラスチックは透過するが金属は透過しないため、侵入者検知装置 1 を車両内に設置して使用する際は、車両のボディを形成する金属部分によりドップラーセンサー 2 の検知できない領域（死角）が存在することになる。しかし、ドップラーセンサー 2 は、車両に加えられた振動については確実に検知することができる。

#### 【0132】

そこで、ID 認証のトリガーとして、ドップラーセンサー 2 による接近の検知と、車両に加えられる振動の検知との両方を、段階的に利用することもできる。例えば、ID 認証の第一のトリガーとしてドップラーセンサー 2 による接近の検知を用い、ID 認証の第二のトリガーとしてドップラーセンサー 2 による車両に加えられる振動の検知を用いる方式により、死角からの物体の接近についても、車両のドアを開けるなどの車両に加えられる振動を検知することにより、確実に検知し、ID 認証を行うことができる。

#### 【0133】

この方法を用いて、第二のトリガーである、車両に振動が加えられたことの検知に応答して、ID 認証を開始した場合、認証処理部 3 により ID 認証が不適合であると判断され

た後に、威嚇処理が実行される。すなわち、車両に振動が加えられたことを検知してから I D 認証に要する時間が経過する間は威嚇処理は行われず、接近者がユーザであった場合に誤って威嚇処理が行われることを防止することができる。

【0134】

上記の方法によれば、I D 認証処理はより確実に行われるため、より確実な防犯システムを確立することができる。

【0135】

また、上記のような方法によれば、車両に振動が加えられた際にドップラーセンサー 2 によりその振動を検知し、その検知結果に応答して I D 認証が行われるため、侵入者を高感度で検知でき、侵入者検知装置 1 の侵入者検知の信頼性を向上しながら、I D 認証のための無線通信を効率よく減らすことができ、無線通信に伴う消費電力を更に抑制することができる。

【産業上の利用可能性】

【0136】

本発明によると、車両、建物等への侵入者を検知する侵入者検知装置において、物体の接近がユーザであるか侵入者であるかの判断を行う I D 認証処理を、十分かつ無駄無く行うことができ、また、侵入者に対して威嚇処理を実行する侵入者侵入者威嚇装置にも適用できる。

【図面の簡単な説明】

【0137】

【図 1】 本発明の一実施形態に係る侵入者検知装置の構成を示すブロック図である。

【図 2】 図 1 の侵入者検知装置において自動的に侵入者検知装置 1 の警戒状態の設定が行われる手順を示した説明図である。

【図 3】 図 1 の侵入者検知装置における処理の他の手順を示すフローチャート図である。

【図 4】 図 1 の侵入者検知装置において自動的に侵入者検知装置の警戒状態の解除が行われる手順を示した説明図である。

【図 5】 図 1 の侵入者検知装置における処理の手順を示すフローチャート図である。

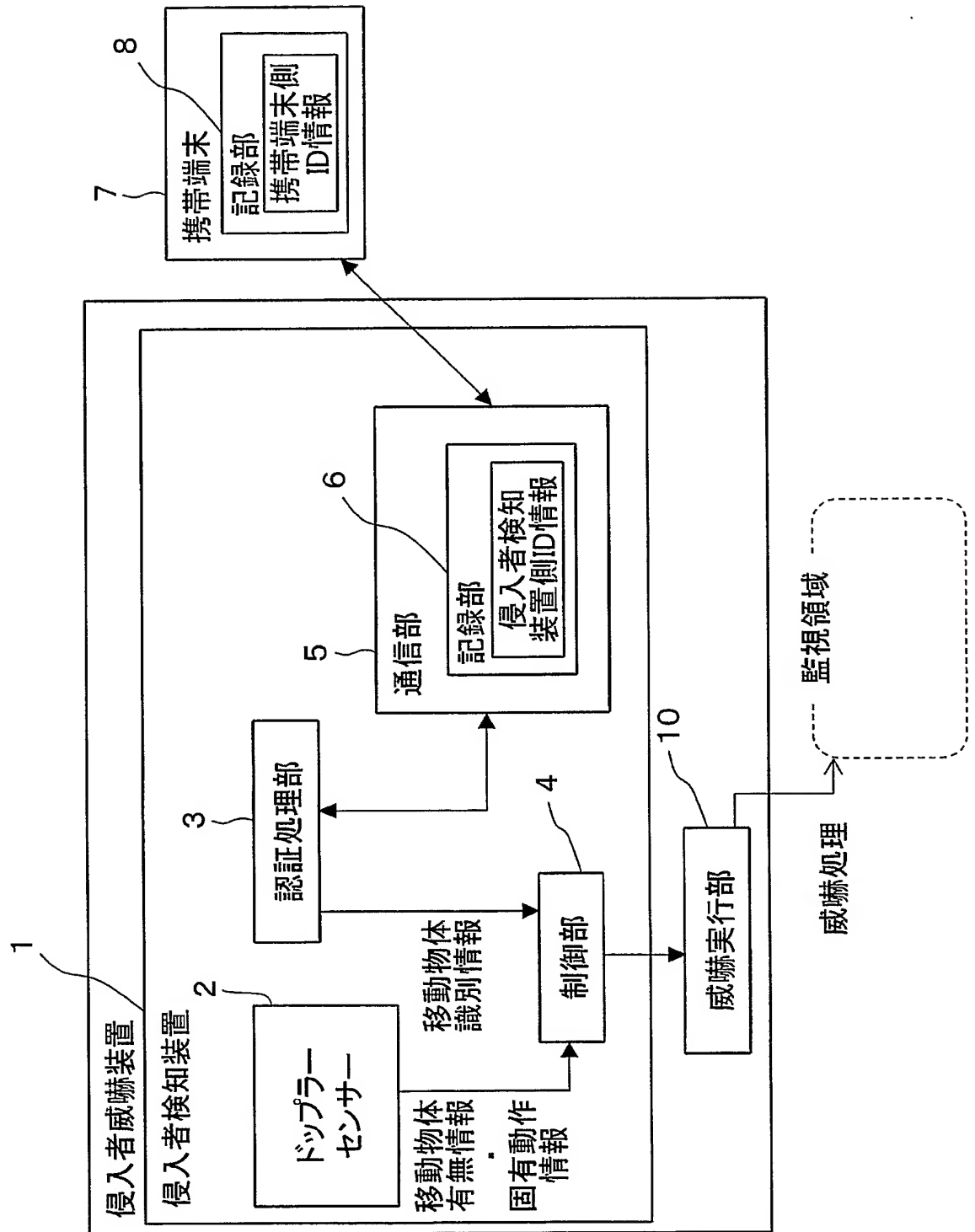
【図 6】 図 1 の侵入者検知装置における処理の他の手順を示すフローチャート図である。

【符号の説明】

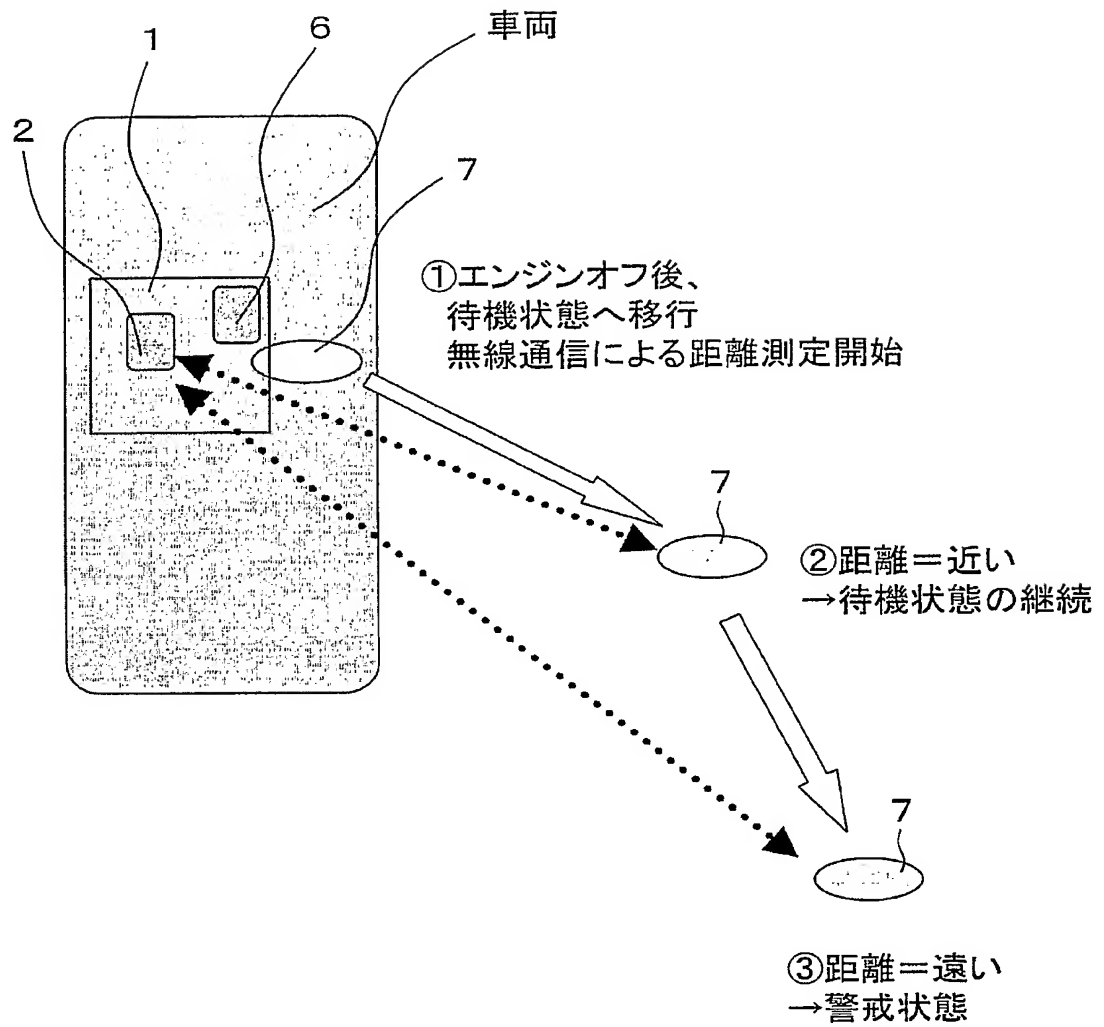
【0138】

- 1 侵入者検知装置
- 2 ドップラーセンサー
- 3 認証処理部（認証処理手段）
- 4 制御部（制御装置）
- 5 通信部（通信手段）
- 6 記録部
- 7 携帯端末
- 8 記録部
- 10 威嚇実行部（威嚇実行手段）

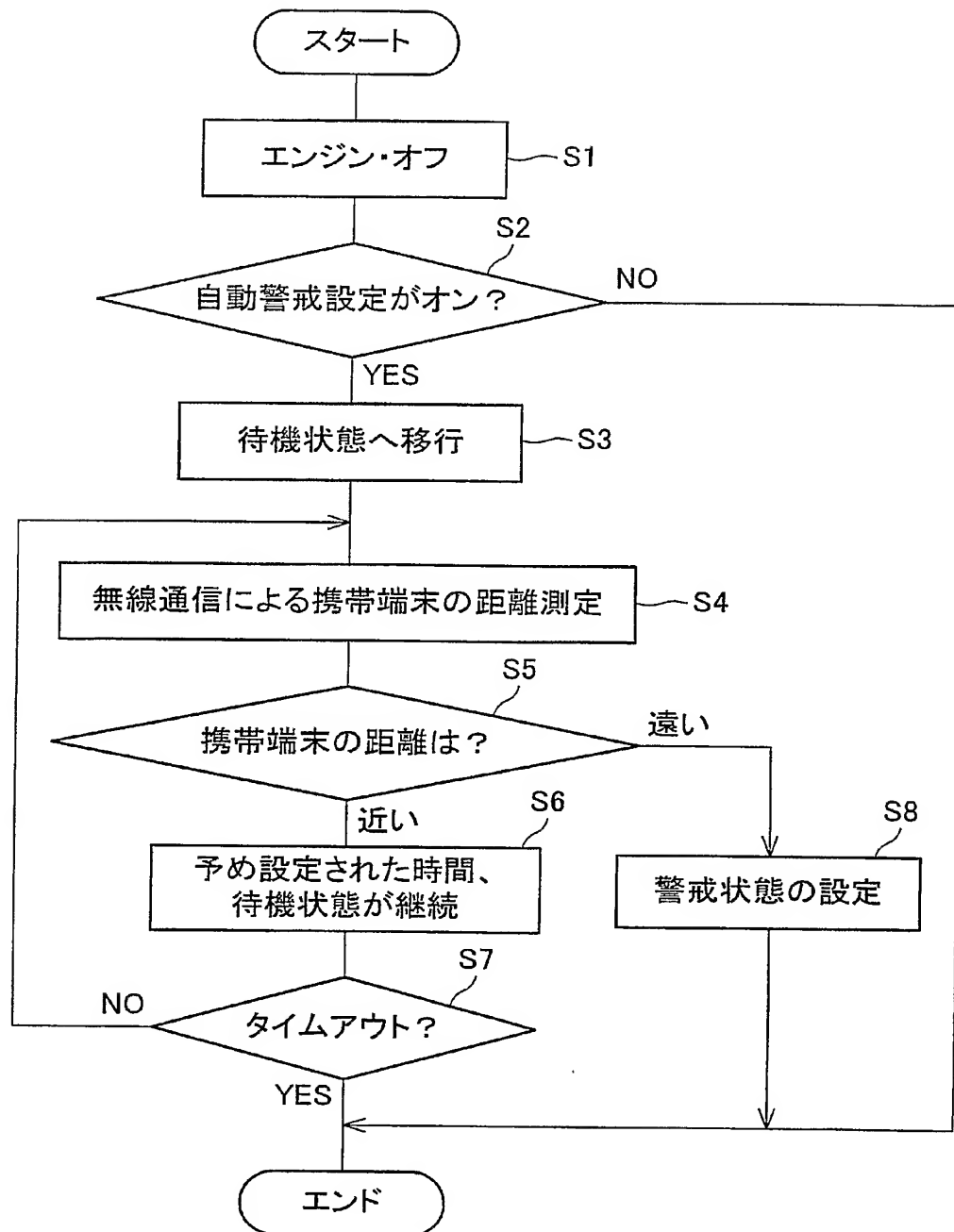
【書類名】 図面  
【図 1】



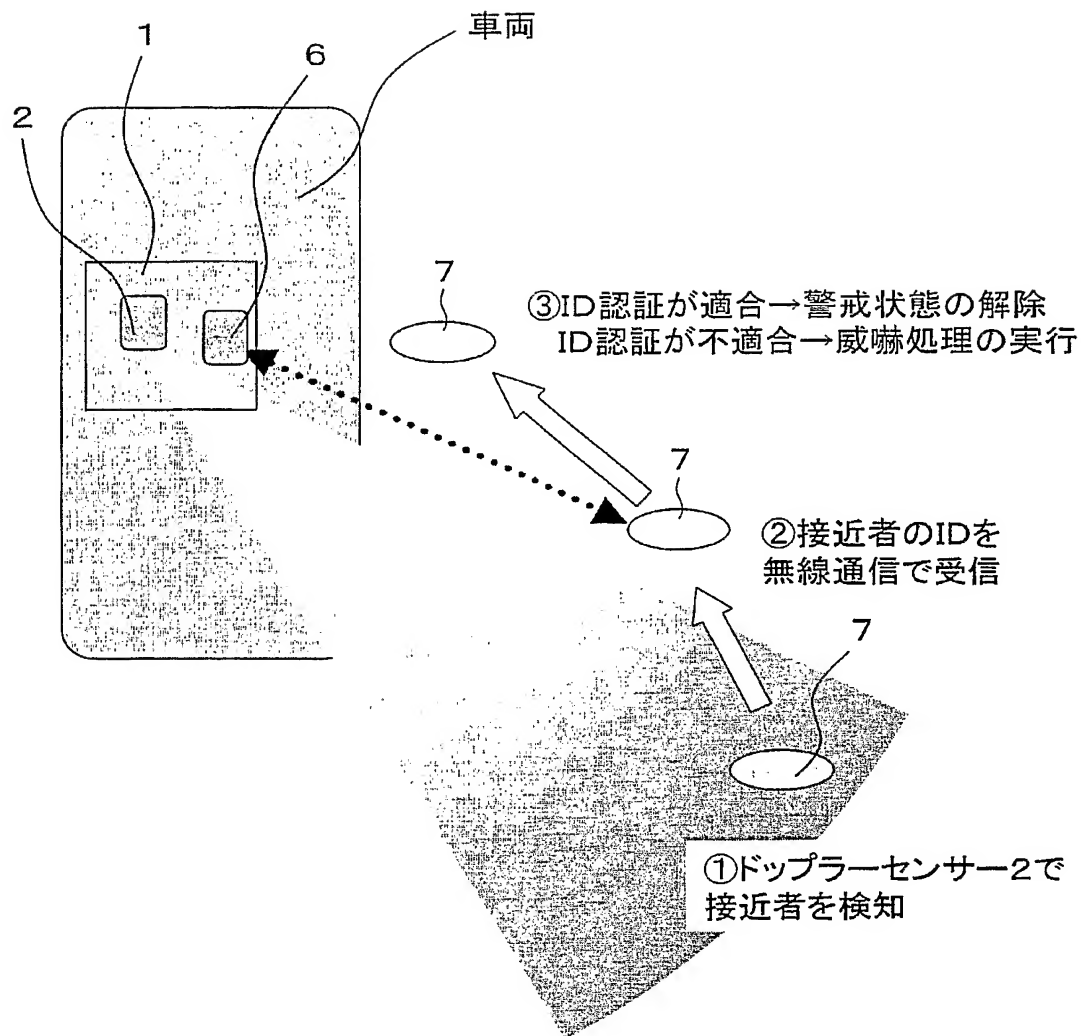
【図 2】



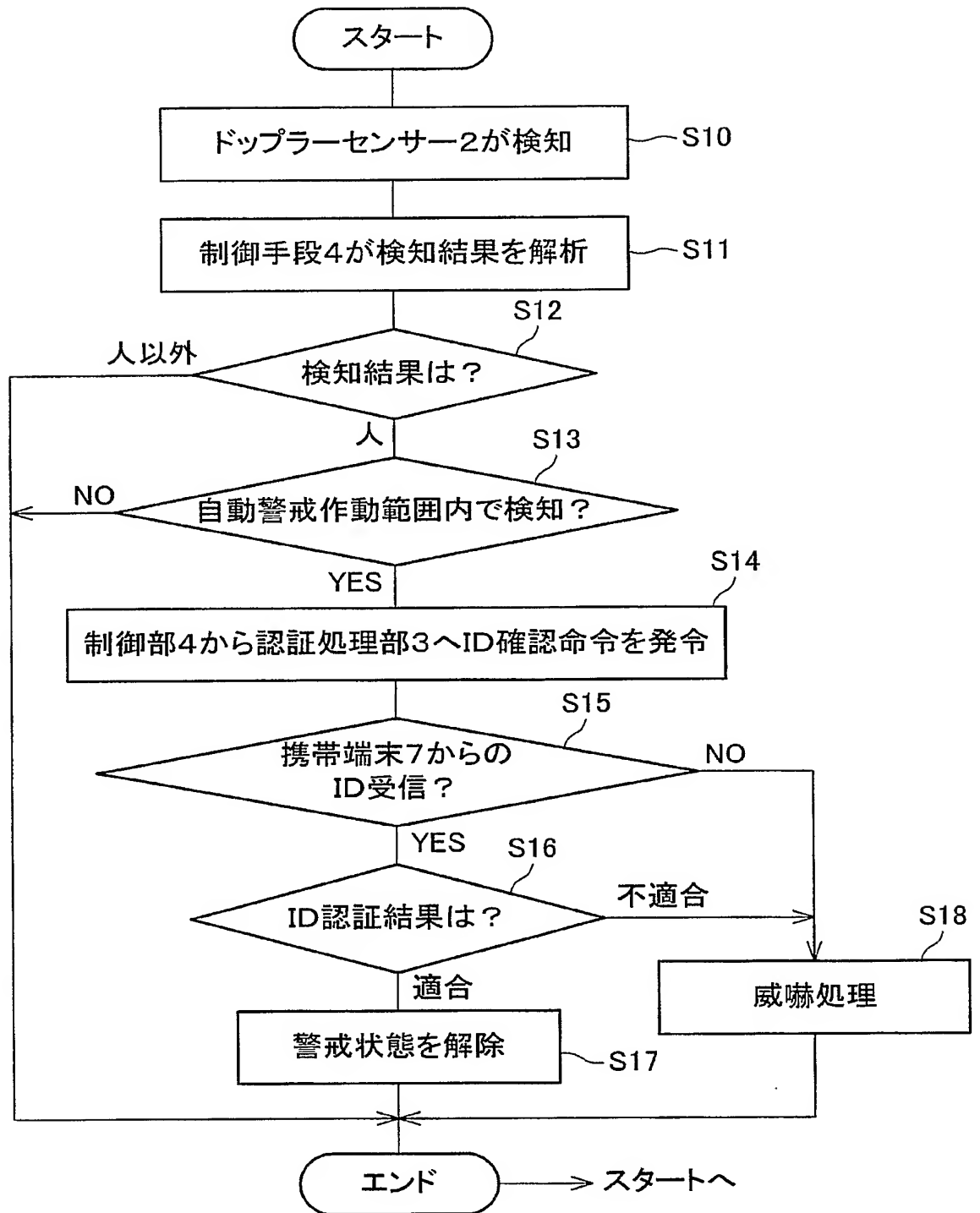
【図 3】



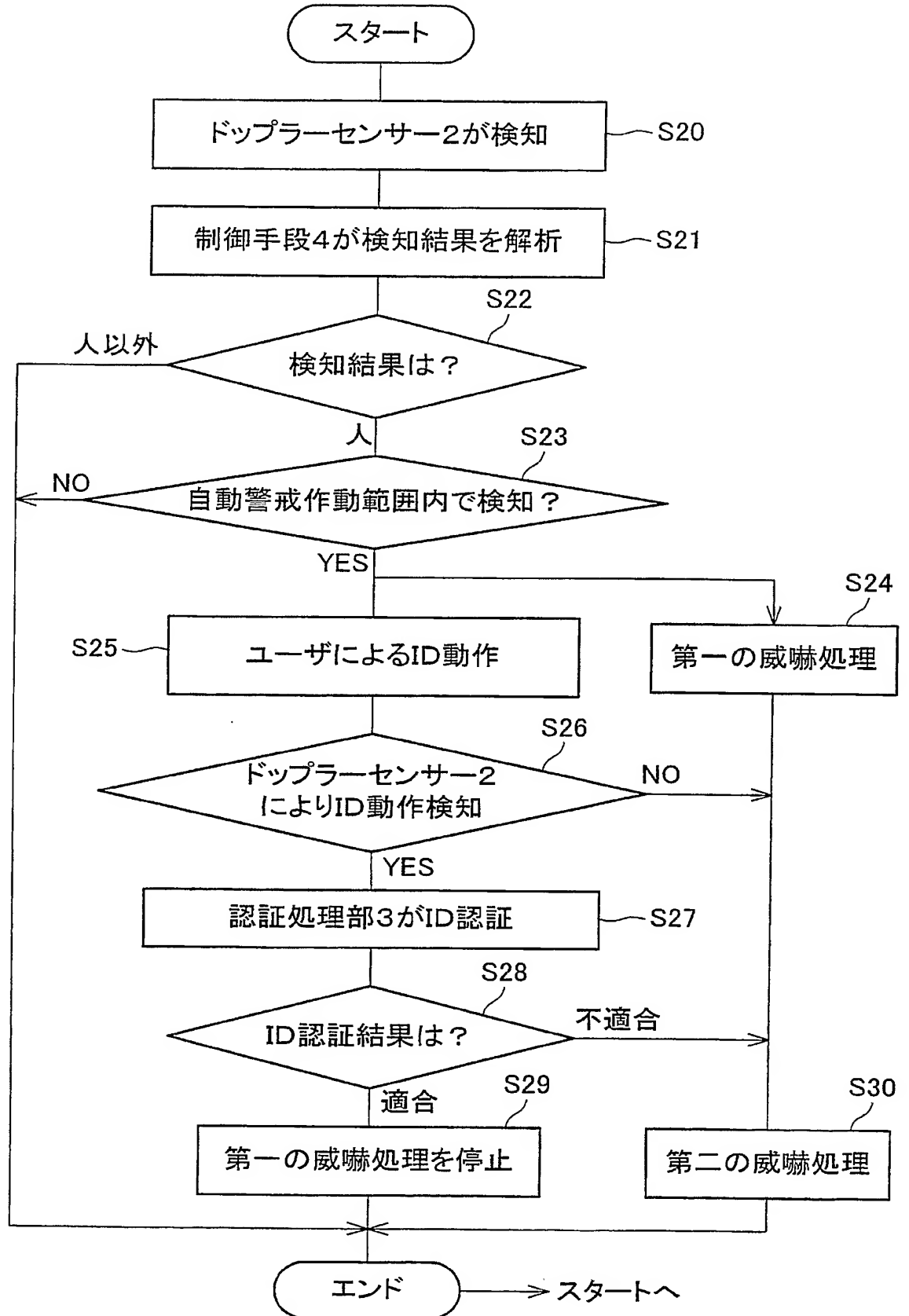
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 侵入者検知装置において、侵入者検知装置の警戒状態設定、解除、あるいは威嚇処理の実行を行うために必要な I D 認証を、装置の多容量化・高コスト化を生じること無く、十分かつ無駄無く行うことができることを目的としている。

【解決手段】 ドップラーセンサー 2 により送波されるマイクロ波の被検知物への反射により生成される反射波の変化を、ドップラーセンサー 2 自身が受信して物体の移動を検知すると、認証処理部 3 が I D 認証処理を行い、認証処理手段の出力に基づいて、制御部 4 が威嚇実行部 1 0 に威嚇処理の実行命令を行う。

【選択図】 図 1

特願 2 0 0 4 - 0 7 3 3 3 5

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 2 9 4 5 ]

1. 変更年月日

2 0 0 0 年 8 月 1 1 日

[変更理由]

住所変更

住 所

京都市下京区塩小路通堀川東入南不動堂町 8 0 1 番地

氏 名

オムロン株式会社